



THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Group Art Unit: 2431
Examiner: Mr. Longbit Chai

In re PATENT APPLICATION of:

Applicant(s) : Yunchuan QIN et al.

Serial No. : 10/594,299

Filed : September 26, 2006

For : SECRET FILE ACCESS AUTHORIZATION
SYSTEM WITH FINGERPRINT LIMITATION

Attorney Ref. : SHA 142NP

)
)
)
)
) **APPEAL BRIEF**
)
)
)
)
)

August 10, 2009

Attn: Mail Stop Appeal Brief-Patents

Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450

Sir:

INTRODUCTION

This is an Appeal to the Board of Patent Appeals and Interferences from the decision, in an Office Action dated October 13, 2009 (and hereafter called the "Final Rejection"), finally rejecting all of the claims (that is, claims 1-61). A Notice of Appeal and a Petition for an extension of time were filed on April 13, 2010, thus making the original due-date for the present Appeal Brief June 13, 2010. A further petition for an extension of time is being filed concurrently.

A fee of \$ 515 is also being submitted concurrently. Should this remittance be accidentally missing, however, or should any additional fees be needed, the Director may charge such fees to our Deposit Account number 18-0002.

08/11/2010 SMOHAMME 00000035 10594299

01 FC:2402

270.00 OP

(i) REAL PARTY IN INTEREST

The real party in interest in this appeal is the Assignee, SHANGHAI SANLEN INFO SECURITY CO., LTD., having an office at Rooms 1702-03, Gangtai Square, 700 Yanan (E) Road, Huangpu District, Shanghai, 200001, China.

(ii) RELATED APPEALS AND INTERFERENCES

To the best of the knowledge and belief of the undersigned attorney, there are no prior or pending appeals, interferences, or judicial proceedings which may be related to, directly affect or be directly affected by, or have a bearing on the Board's decision in the pending appeal.

(iii) STATUS OF THE CLAIMS

Claims 1-61 are pending in this application. No claims have been cancelled and no claims have been allowed. All of the pending claims are involved in this appeal.

(iv) STATUS OF AMENDMENTS

A Response After Final Rejection (which made no changes in the claims) was filed on March 15, 2010. An Advisory Action dated April 5, 2010 reported that the claims remained finally rejected.

An Amendment is being filed currently, together with a request that it be entered for purposes of appeal, to correct an error in claim 1. It is noted that the claims appendix to this Brief includes the requested correction.

(v) SUMMARY OF CLAIMED SUBJECT MATTER

The present application discloses techniques for protecting secret files from an unauthorized access. It does this by limiting access to the secret files to a particular environment, such as a particular computer (see the passage at page 2 of the application, lines 2-13) and a particular time period (see page 2, lines 14-20).

Figure 7 of the application's drawings shows a system that includes an authorization module 10, an encryption module 20, a certification module 30, and a user module 40. The details of the authorization module 10 are shown in Figure 3. In Figure 3, the authorization module 10 is included in an authorization server 1, and includes a password fingerprint unit 101, an environment fingerprint sampling unit 102, and a time fingerprint sampling unit 103 that are coupled in parallel to an authorization unit 104. The password fingerprint unit 101 is provided to receive a password (page 6, lines 26-28). The environment fingerprint sampling unit 102 receives data from a designated environment, such as the MAC address of a network card or the serial number of a hard drive, to create an environmental fingerprint (page 6, lines 28-31). The time fingerprint sampling unit 103 generates a time fingerprint based on the current time and a time limitation designated by an administrator (page 6, line 30 to page 7, line 2). The authorization unit 104 generates an authorization secret key 5 according to the fingerprints (page 7, lines 2-7). The fingerprint sampling units 101, 102, and 103 can be merged into a fingerprint template 6 (page 7, lines 9-13).

The encryption module 20, which is shown in Figure 4, is provided in an encryption server 2. It includes a secret key generation unit 201, which receives the authorization secret key 5 and generates a decryption secret key 7 (page 7, lines 17-20). The encryption module

20 also includes an encryption unit 202, which receives a secret file 8 that is to be encrypted and outputs an encrypted secret file 9 (page 7, lines 20-26).

The certification module 30, which is shown in Figure 5, is provided in a certification server 3. It includes certification units 301, 302, and 303, which are coupled to a certification interface unit 304 (page 7, lines 26-32). The certification interface unit 304 also receives the decryption secret key and an authorization secret key 5' that has been sent for certification by a client machine, and generates a certified decryption key 7' if all of the fingerprints are satisfactory (page 8, lines 4-23).

Figure 6 shows the user module 40, which is provided in a user machine 4. It receives the authorization secret key 5 and presents it (as 5' in Figure 5) for certification, and receives the certified decryption secret key 7' if the certification attempt passes (page 8, line 24 to page 9, line 4). The certified decryption secret key 7' is necessary for decryption by a kernel encryption/decryption unit 402, which uses the key 7' to decrypt and encrypt a secret file 9 (page 9, lines 4-11).

The following **claim chart** shows an example of how the claims that will be separately argued later in this brief can be read on the disclosure.

1. A secret file access authorization system with fingerprint limitation, comprising:
an authorization server (1; page 6, lines 22-23) provided with an authorization module (10; page 6, lines 22-23), which provides a fingerprint template (6; page 7, lines 9-13) and an authorization secret key (5; page 7, lines 2-7), the authorization module including a password fingerprint unit (101; page 7, lines 23-26), an environment fingerprint sampling unit (102; page 7, lines 23-26), and a time fingerprint sampling unit (103; page 7, lines 23-26), which are set in parallel, as well as an authorization unit (104; page 7; lines 23-26);

an encryption server (2; page 7, lines 17-18) provided with an encryption module (20; page 7, lines 17-18), which generates a decryption secret key (7; page 7, lines 20-22) by accepting the authorization secret key provided by the authorization module (page 7; lines 20-22), and produces encrypted secret files (9; page 7, lines 22-24) by encrypting secret files to be encrypted (8; page 7, lines 22-24);

a certification server (3; page 7, lines 27-28) provided with a certification module (30; page 7, lines 27-28), which accepts the fingerprint template provided by the authorization module (page 7, line 28 to page 8, line 4), accepts the decryption secret key provided by the encryption module (page 8, lines 19-24) and the authorization secret key claiming certification (page 8, lines 6-9) that is sent by a client, and judges and confirms by providing a certified decryption secret key (7; page 8, lines 19-24); and

at least one client machine (4; page 8, lines 24-25), each of which is provided with a user module (40; page 8, lines 24-25), which embeds a kernel encryption/decryption unit (402; page 8, lines 25-29) into a corresponding operation system kernel of the client, accepts the authorization secret key provided by the authorization module (page 8, lines 29-32) and the decryption secret key provided by the encryption module, sends the claiming of certification respectively to the certification module, opens the encryption/decryption unit with a certified authorization secret key and the certified decryption secret key which is returned after the certification module makes the certification (page 8, line 29 to page 9, line 4), and reads/writes the encrypted secret files (page 9, lines 5-8).

61. A secret file access authorization system with fingerprint limitation according to claim 1, wherein the environment fingerprint sampling unit determines whether a request for

decryption of one of the encrypted secret files originated from a client machine that is authorized to decrypt said one of the encrypted secret files (page 6, lines 28-31), and wherein the time signature sampling unit determines whether said request for decryption has occurred during a limited time window set for authorized decryption (page 2, lines 14-20 and page 6, line 31 to page 7, line 2).

(vi) GROUND OF REJECTION TO BE REVIEWED ON APPEAL

All of the pending claims stand rejected for obviousness on the basis of published US application 2002/0010679 to Felsher (and items of prior art that are incorporated in Felsher by reference) in view of published US application 2003/0018892 to Tello.

(vii) ARGUMENT

Claim 1 provides that an authorization module includes “a password fingerprint unit, an environment fingerprint sampling unit, and a time fingerprint sampling unit, which are set in parallel.” The Final Rejection takes the position that Felsher discloses such an authorization module, and refers to Felsher’s paragraphs [0087] and [0354].

Felsher’s paragraph [0087] summarizes the disclosure of one of the many items of prior art that Felsher incorporates by reference. Paragraph [0087] says that, in one embodiment of the prior art, “verification includes locking the digital information to the requesting computer system by comparing a generated digital fingerprint associated with the digital information to a digital fingerprint previously generated which is unique to the requesting computer system.”

Felsher's paragraph [0354] advises that the authenticity of a user

... may be verified with a hardware token, such as the RSA SecurID hardware token. These tokens are small, handheld devices containing microprocessors that calculate and display unpredictable codes. These codes change at a specified interval, typically 60 seconds.

Felsher's paragraph [0354] goes on to say that the user enters the password that is currently displayed on the SecurID device and, if the password that the user enters does not match what is currently being displayed, the password from the previous 60-second interval is also checked in case there was a delay in typing and transmission.

Thus Felsher's paragraphs [0087] and [0354] disclose comparing a fingerprint associated with requested information to a fingerprint which is unique to the requesting computer system (Felsher's paragraph [0087]), and a hardware token with a password that changes with time (Felsher's paragraph [0354]). But Felsher's paragraph [0087] describes just one reference out what appears to be well over a hundred that Felsher has incorporated by reference. But there is no apparent reason why an ordinarily skilled person would select the particular technique described in Felsher's paragraph [0087] instead of the many other techniques disclosed in other items of prior art that Felsher has incorporated by reference, and use it in combination with the SecurID hardware token discussed in Felsher's paragraph [0354]. The rejection is somewhat like a rejection based on an engineering handbook that covers many related topics.

A SecurID hardware token is used for providing two-factor authentication. The user must combine his secret Personal Identification Number (PIN) with the token code that changes every sixty seconds in order to access a secret file. The SecurID token does not sample an environment fingerprint. Instead, it generates an unpredictable code every sixty

seconds using the same algorithm that is employed at an authorization server regardless of the token's environment. As long as a user holds a legal token and a legal PIN number, the user will be able to access a secret file any time and anywhere. Accordingly, it cannot reasonably be said that a SecurID hardware token is an "environment fingerprint sampling unit" as recited in claim 1. Nor it is a "time fingerprint sampling unit" as recited in the claim, since it simply changes the code every sixty seconds. This cannot be reasonably be said to sample a "time fingerprint" as the term is used in the present application.

Furthermore, claim 1 recites "at least one client machine." If an ordinarily skilled person wanted to employ a SecurID hardware token to supply a user with a changeable password, it seems likely that the ordinarily skilled person would think that the SecurID token should be available at the client's machine, not at an authorization module as specified in claim 1.

The techniques disclosed in the present application permit an administrator to designate one or more valid environments based on practical needs, and the administrator can also set a time window and require a password. This provides three-way protection for secret files, since the secret files cannot be accessed unless all three kinds of fingerprints are certified.

The Tello reference is directed to an arrangement that permits a computer to be booted only by authorized personnel. Tello does not make up for the shortcomings of Felsher that are discussed above, so the rejection of claim 1 should be reversed.

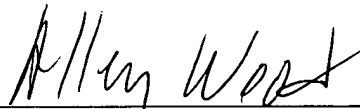
The remaining claims depend from claim 1 and recite additional limitations that further define the invention, so they are automatically patentable along with claim 1. Nevertheless, dependent claim 61 will now be briefly discussed.

Claim 61 provides that “the environment fingerprint sampling unit determines whether a request for decryption of one of the encrypted secret files originated from a client machine that is authorized to decrypt said one of the encrypted secret files,” and that “the time signature sampling unit determines whether said request for decryption has occurred during a limited time window set for authorized decryption.” These features are not suggested by the references. In particular, a periodically changing code that is displayed on a SecurID token has nothing to do with whether a request for decryption “has occurred during a limited time window set for authorized decryption.”

CONCLUSION

For the foregoing reasons, it is respectfully submitted that the rejected claims are patentable over the Felsher and Tello references. The Examiner’s rejection of these claims should therefore be reversed.

Respectfully submitted,

A handwritten signature in black ink, appearing to read "Allen Wood", is written over a horizontal line.

Allen Wood (Reg. No. 28,134)
Customer No. 23995
RABIN & BERDO, P.C.
Telephone: (202) 326-0222
Telefax: (202) 371-8976

AW/ng

(viii) CLAIMS APPENDIX

The claims involved in this appeal are presented below (it being noted that the following claims include corrections to claim 1 that are presented in an Amendment that is being filed concurrently with this Brief).

1. A secret file access authorization system with fingerprint limitation, comprising:

an authorization server provided with an authorization module, which provides a fingerprint template and an authorization secret key, the authorization module including a password fingerprint unit, an environment fingerprint sampling unit, and a time fingerprint sampling unit, which are set in parallel, as well as an authorization unit;

an encryption server provided with an encryption module, which generates a decryption secret key by accepting the authorization secret key provided by the authorization module, and produces encrypted secret files by encrypting secret files to be encrypted;

a certification server provided with a certification module, which accepts the fingerprint template provided by the authorization module, accepts the decryption secret key provided by the encryption module and the authorization secret key claiming certification that is sent by a client, and judges and confirms by providing a certified decryption secret key; and

at least one client machine, each of which is provided with a user module, which embeds a kernel encryption/decryption unit into a corresponding operation system kernel of the client, accepts the authorization secret key provided by the authorization module and the decryption secret key provided by the encryption module, sends the claiming of certification respectively to the certification module, opens the encryption/decryption unit with a certified authorization secret key and the certified decryption secret key which is returned after the certification module makes the certification, and reads/writes the encrypted secret files.

2. A secret file access authorization system with fingerprint limitation according to claim 1, wherein the authorization server, the encryption server, and the certification server are merged to constitute a system server, which is provided with the authorization module, the encryption module, and the certification module.

3. A secret file access authorization system with fingerprint limitation according to claim 1, wherein the authorization server and the encryption server are merged to constitute an authorization-and-encryption server, which is provided with the authorization module and the encryption module.

4. A secret file access authorization system with fingerprint limitation according to claim 1, wherein the authorization server and the certification server are merged to constitute an authorization-and-certification server, which is provided with the authorization module and the certification module.

5. A secret file access authorization system with fingerprint limitation according to claim 1, wherein the encryption server and the certification server are merged to constitute an encryption-and-certification server, which is provided with the encryption module and the certification module.

6. A secret file access authorization system with fingerprint limitation according to claim 1, wherein the password fingerprint unit, the environment fingerprint sampling unit, and the time fingerprint sampling unit are set in parallel respectively by bidirectional programs; and wherein the authorization unit provides the authorization secret key, while the password fingerprint unit, the environment fingerprint sampling unit, and the time fingerprint sampling unit that are set in parallel provide the fingerprint template.

7. A secret file access authorization system with fingerprint limitation according to claim 6, wherein the authorization secret key is a binary string of a certain length.

8. A secret file access authorization system with fingerprint limitation according to claim 7, wherein the authorization secret key is put into an authorized entity.

9. A secret file access authorization system with fingerprint limitation according to claim 6, wherein the fingerprint template is a binary string of a certain length.

10. A secret file access authorization system with fingerprint limitation according to claim 1, wherein the encryption module includes a secret key generation unit and an encryption unit, which are linked in sequence by programs; wherein the secret key generation unit provides the decryption secret key after accepting the authorization secret key provided by the authorization module; and wherein the encryption unit accepts the input of secret files to be encrypted, and produces the encrypted secret files by using the decryption secret key provided by the secret key generation unit.

11. A secret file access authorization system with fingerprint limitation according to claim 10, wherein the encryption unit accepts the input of the secret files to be encrypted, and produces the encrypted secret files by using the authorization secret key.

12. A secret file access authorization system with fingerprint limitation according to claim 10, wherein the encryption unit accepts the input of the secret files to be encrypted, and produces the encrypted secret files by using the decryption secret key and the authorization secret key at the same time.

13. A secret file access authorization system with fingerprint limitation according to claim 1, wherein the certification module includes an environment fingerprint certification unit, a password fingerprint certification unit, and a time fingerprint certification unit set in parallel by accepting the fingerprint template provided by the authorization module; wherein a certification interface unit is linked with them by bidirectional programs, and also accepts the decryption secret key provided by the encryption module and a certification secret key from the user module claiming certification respectively, and provides the certified decryption secret key for the user module.

14. A secret file access authorization system with fingerprint limitation according to claim 1, wherein the user module includes an application unit, a kernel encryption/decryption unit and an input/output unit, which are linked in sequence by bidirectional programs, as well as an authorization input unit, which accepts the authorization secret key and sends it into the

kernel encryption/decryption unit; wherein the kernel encryption/decryption unit provides the authorization secret key claiming certification for a certification module, and accepts a certified decryption secret key sent by the certification module; wherein the input/output unit is coupled with the encrypted secret files bidirectionally; wherein the kernel encryption/decryption unit is embedded in the operation system kernel.

15. A secret file access authorization system with fingerprint limitation according to claim 14, wherein the operation system is Microsoft Windows 95/98/ME/NT/2000/XP/2003 Server or Linux/Unix or Pocket, Symbian OS, Windows CE embedded operation system or Mac OS or Sun OS, Novell netware and other server or network operation systems.

16. A secret file access authorization system with fingerprint limitation according to claim 14, wherein a program used by the application unit is Microsoft Office and its components or other desktop applications or embedded applications.

17. A secret file access authorization system with fingerprint limitation according to claim 2, wherein the authorization module includes the password fingerprint unit, the environment fingerprint sampling unit, the time fingerprint sampling unit, and the authorization unit; wherein the password fingerprint unit, the environment fingerprint sampling unit, and the time fingerprint sampling unit are set in parallel respectively by bidirectional programs; wherein the authorization unit provides the authorization secret key, while the password fingerprint unit, the environment fingerprint sampling unit, and the time fingerprint sampling unit provide the fingerprint template.

18. A secret file access authorization system with fingerprint limitation according to claim 3, wherein the authorization module includes the password fingerprint unit, the environment fingerprint sampling unit, the time fingerprint sampling unit, and the authorization unit; wherein the password fingerprint unit, the environment fingerprint sampling unit, and the time fingerprint sampling unit are set in parallel respectively by bidirectional programs; wherein the authorization unit provides the authorization secret key,

while the password fingerprint unit, the environment fingerprint sampling unit, and the time fingerprint sampling unit that are set in parallel provide the fingerprint template.

19. A secret file access authorization system with fingerprint limitation according to claim 4, wherein the authorization module includes the password fingerprint unit, the environment fingerprint sampling unit, the time fingerprint sampling unit, and the authorization unit; wherein the password fingerprint unit, the environment fingerprint sampling unit, and the time fingerprint sampling unit are set in parallel respectively by bidirectional programs; wherein the authorization unit provides the authorization secret key, while the password fingerprint unit, the environment fingerprint sampling unit, and the time fingerprint sampling unit provide the fingerprint template.

20. A secret file access authorization system with fingerprint limitation according to claim 5, wherein the authorization module includes the password fingerprint unit, the environment fingerprint sampling unit, the time fingerprint sampling unit, and the authorization unit; wherein the password fingerprint unit, the environment fingerprint sampling unit, and the time fingerprint sampling unit are set in parallel respectively by bidirectional programs; wherein the authorization unit provides the authorization secret key, while the password fingerprint unit, the environment fingerprint sampling unit, and the time fingerprint sampling unit that are set in parallel provide the fingerprint template.

21. A secret file access authorization system with fingerprint limitation according to claim 17, wherein the authorization secret key is a binary string of a certain length.

22. A secret file access authorization system with fingerprint limitation according to claim 18, wherein the authorization secret key is a binary string of a certain length.

23. A secret file access authorization system with fingerprint limitation according to claim 19, wherein the authorization secret key is a binary string of a certain length.

24. A secret file access authorization system with fingerprint limitation according to claim 20, wherein the authorization secret key is a binary string of a certain length.

25. A secret file access authorization system with fingerprint limitation according to claim 21, wherein the authorization secret key is put into an authorized entity.

26. A secret file access authorization system with fingerprint limitation according to claim 22, wherein the authorization secret key is put into an authorized entity.

27. A secret file access authorization system with fingerprint limitation according to claim 23, wherein the authorization secret key is put into an authorized entity.

28. A secret file access authorization system with fingerprint limitation according to claim 24, wherein the authorization secret key is put into an authorized entity.

29. A secret file access authorization system with fingerprint limitation according to claim 17, wherein the fingerprint template is a binary string of a certain length.

30. A secret file access authorization system with fingerprint limitation according to claim 18, wherein the fingerprint template is a binary string of a certain length.

31. A secret file access authorization system with fingerprint limitation according to claim 19, wherein the fingerprint template is a binary string of a certain length.

32. A secret file access authorization system with fingerprint limitation according to claim 20, wherein the fingerprint template is a binary string of a certain length.

33. A secret file access authorization system with fingerprint limitation according to claim 2, wherein the encryption module includes a secret key generation unit and an encryption unit, which are linked in sequence by programs; wherein the secret key generation unit provides the decryption secret key after accepting the authorization secret key provided

by the authorization module; and wherein the encryption unit accepts the input of secret files to be encrypted, and produces the encrypted secret files by using the decryption secret key provided by the secret key generation unit.

34. A secret file access authorization system with fingerprint limitation according to claim 3, wherein the encryption module includes a secret key generation unit and an encryption unit, which are linked in sequence by programs; wherein the secret key generation unit provides the decryption secret key after accepting the authorization secret key provided by the authorization module; and wherein the encryption unit accepts the input of secret files to be encrypted, and produces the encrypted secret files by using the decryption secret key provided by the secret key generation unit.

35. A secret file access authorization system with fingerprint limitation according to claim 4, wherein the encryption module includes a secret key generation unit and an encryption unit, which are linked in sequence by programs; wherein the secret key generation unit provides the decryption secret key after accepting the authorization secret key provided by the authorization module; and wherein the encryption unit accepts the input of secret files to be encrypted, and produces the encrypted secret files by using the decryption secret key provided by the secret key generation unit.

36. A secret file access authorization system with fingerprint limitation according to claim 5, wherein the encryption module includes a secret key generation unit and an encryption unit, which are linked in sequence by programs; wherein the secret key generation unit provides the decryption secret key after accepting the authorization secret key provided by the authorization module; and wherein the encryption unit accepts the input of secret files to be encrypted, and produces the encrypted secret files by using the decryption secret key provided by the secret key generation unit.

37. A secret file access authorization system with fingerprint limitation according to claim 33, wherein the encryption unit accepts the input of the secret files to be encrypted, and produces the encrypted secret files by using the authorization secret key.

38. A secret file access authorization system with fingerprint limitation according to claim 34, wherein the encryption unit accepts the input of the secret files to be encrypted, and produces the encrypted secret files by using the authorization secret key.

39. A secret file access authorization system with fingerprint limitation according to claim 35, wherein the encryption unit accepts the input of the secret files to be encrypted, and produces the encrypted secret files by using the authorization secret key.

40. A secret file access authorization system with fingerprint limitation according to claim 36, wherein the encryption unit accepts the input of the secret files to be encrypted, and produces the encrypted secret files by using the authorization secret key.

41. A secret file access authorization system with fingerprint limitation according to claim 33, wherein the encryption unit accepts the input of the secret files to be encrypted, and produces the encrypted secret files by using the decryption secret key and the authorization secret key at the same time.

42. A secret file access authorization system with fingerprint limitation according to claim 34, wherein the encryption unit accepts the input of the secret files to be encrypted, and produces the encrypted secret files by using the decryption secret key and the authorization secret key at the same time.

43. A secret file access authorization system with fingerprint limitation according to claim 35, wherein the encryption unit accepts the input of the secret files to be encrypted, and produces the encrypted secret files by using the decryption secret key and the authorization secret key at the same time.

44. A secret file access authorization system with fingerprint limitation according to claim 36, wherein the encryption unit accepts the input of the secret files to be encrypted, and

produces the encrypted secret files by using the decryption secret key and the authorization secret key at the same time.

45. A secret file access authorization system with fingerprint limitation according to claim 2, wherein the certification module includes an environment fingerprint certification unit, a password fingerprint certification unit, and a time fingerprint certification unit set in parallel by accepting the fingerprint template provided by the authorization module; and wherein a certification interface unit is linked with them by bidirectional programs, which also accepts the decryption secret key provided by the encryption module and the certification secret key from the user module claiming certification respectively, and provides the certified decryption secret key for the user module.

46. A secret file access authorization system with fingerprint limitation according to claim 3, wherein the certification module includes an environment fingerprint certification unit, a password fingerprint certification unit, and a time fingerprint certification unit set in parallel by accepting the fingerprint template provided by the authorization module; and wherein a certification interface unit is linked with them by bidirectional programs, which also accepts the decryption secret key provided by the encryption module and the certification secret key from the user module claiming certification respectively, and provides the certified decryption secret key for the user module.

47. A secret file access authorization system with fingerprint limitation according to claim 4, wherein the certification module includes an environment fingerprint certification unit, a password fingerprint certification unit, and a time fingerprint certification unit set in parallel by accepting the fingerprint template provided by the authorization module; and wherein a certification interface unit is linked with them by bidirectional programs, which also accepts the decryption secret key provided by the encryption module and the certification secret key from the user module claiming certification respectively, and provides the certified decryption secret key for the user module.

48. A secret file access authorization system with fingerprint limitation according to claim 5, wherein the certification module includes an environment fingerprint certification unit, a password fingerprint certification unit, and a time fingerprint certification unit set in parallel by accepting the fingerprint template provided by the authorization module; and wherein a certification interface unit linked with them by the bidirectional programs, which also accepts the decryption secret key provided by the encryption module and the certification secret key from the user module claiming certification respectively, and provides the certified decryption secret key for the user module.

49. A secret file access authorization system with fingerprint limitation according to claim 2, wherein the user module includes an application unit, the kernel encryption/decryption unit, and an input/output unit, which are linked in sequence by bidirectional programs, and an authorization input unit, which accepts the authorization secret key and sends it into the kernel encryption/decryption unit; wherein the kernel encryption/decryption unit provides the authorization secret key claiming certification for the certification module, and accepts the certified decryption secret key sent by the certification module; wherein an input/output unit is coupled with the encrypted secret files bidirectionally; and wherein the kernel encryption/decryption unit is embedded in the operation system kernel.

50. A secret file access authorization system with fingerprint limitation according to claim 3, wherein the user module includes an application unit, the kernel encryption/decryption unit, and an input/output unit, which are linked in sequence by bidirectional programs, and an authorization input unit, which accepts the authorization secret key and sends it into the kernel encryption/decryption unit; wherein the kernel encryption/decryption unit provides the authorization secret key claiming certification for the certification module, and accepts the certified decryption secret key sent by the certification module; and the input/output unit is coupled with the encrypted secret files bidirectionally; and wherein the kernel encryption/decryption unit is embedded in the operation system kernel.

51. A secret file access authorization system with fingerprint limitation according to claim 4, wherein the user module includes an application unit, the kernel encryption/decryption unit, and an input/output unit, which are linked in sequence by bidirectional programs, and an authorization input unit, which accepts the authorization secret key and sends it into the kernel encryption/decryption unit; wherein the kernel encryption/decryption unit provides the authorization secret key claiming certification for the certification module, and accepts the certified decryption secret key sent by the certification module; wherein the input/output unit is coupled with the encrypted secret files bidirectionally; and wherein the kernel encryption/decryption unit is embedded in the operation system kernel.

52. A secret file access authorization system with fingerprint limitation according to claim 5, wherein the user module includes an application unit, the kernel encryption/decryption unit, and an input/output unit, which are linked in sequence by bidirectional programs, and an authorization input unit, which accepts the authorization secret key and sends it into the kernel encryption/decryption unit; wherein the kernel encryption/decryption unit provides the authorization secret key claiming certification for the certification module, and accepts the certified decryption secret key sent by the certification module; wherein the input/output unit is coupled with the encrypted secret files bidirectionally; and wherein the kernel encryption/decryption unit is embedded in the operation system kernel.

53. A secret file access authorization system with fingerprint limitation according to claim 49, wherein the operation system is Microsoft Windows 95/98/ME/NT/2000/XP/2003 Server or Linux/Unix or Pocket, Symbian OS, Windows CE embedded operation system or Mac OS or Sun OS, Novell netware and other server or network operation systems.

54. A secret file access authorization system with fingerprint limitation according to claim 50, wherein the operation system is Microsoft Windows 95/98/ME/NT/2000/XP/2003 Server or Linux/Unix or Pocket, Symbian OS, Windows CE embedded operation system or Mac OS or Sun OS, Novell netware and other server or network operation systems.

55. A secret file access authorization system with fingerprint limitation according to claim 51, wherein the operation system is Microsoft Windows 95/98/ME/NT/2000/XP/2003 Server or Linux/Unix or Pocket, Symbian OS, Windows CE embedded operation system or Mac OS or Sun OS, Novell netware and other server or network operation systems.

56. A secret file access authorization system with fingerprint limitation according to claim 52, wherein the operation system is Microsoft Windows 95/98/ME/NT/2000/XP/2003 Server or Linux/Unix or Pocket, Symbian OS, Windows CE embedded operation system or Mac OS or Sun OS, Novell netware and other server or network operation systems.

57. A secret file access authorization system with fingerprint limitation according to claim 49, wherein a program used by the application unit is Microsoft Office and its components or other desktop applications or embedded applications.

58. A secret file access authorization system with fingerprint limitation according to claim 50, wherein a program used by the application unit is Microsoft Office and its components or other desktop applications or embedded applications.

59. A secret file access authorization system with fingerprint limitation according to claim 51, wherein a program used by the application unit is Microsoft Office and its components or other desktop applications or embedded applications.

60. A secret file access authorization system with fingerprint limitation according to claim 52, wherein a program used by the application unit is Microsoft Office and its components or other desktop applications or embedded applications.

61. A secret file access authorization system with fingerprint limitation according to claim 1, wherein the environment fingerprint sampling unit determines whether a request for decryption of one of the encrypted secret files originated from a client machine that is authorized to decrypt said one of the encrypted secret files, and wherein the time signature

sampling unit determines whether said request for decryption has occurred during a limited time window set for authorized decryption.

(ix) EVIDENCE APPENDIX

No new evidence is being submitted with this Brief.

(x) RELATED PROCEEDINGS APPENDIX

In view of section (ii) of this Brief, no copies of decisions are appended.